HOUSES OF PARLIAMENT
PARLIAMENTARY OFFICE OF SCIENCE & TECHNOLOGY

POSTNOTE

Number 434 April 2013

Managing Online Identity

The Government plans to digitise more public services by 2015 to improve efficiency and reduce costs. As more daily activities, services and transactions are conducted online, increasing amounts of personal data are used on the internet. This POSTnote describes online identity, government projects to secure online access to public services and the issues arising from a more online society.

Overview

- Online services and networks are changing the way people interact socially as well as with businesses and Government.
- New approaches to verify the identity of people and businesses using online services are central to public services that are going digital across Government.
- The Government Digital Service is developing a new way for citizens to assert their identity online, in order to access public services.
- Cybercrime and identity fraud mean that secure online identities are required. Privacy and security remain top concerns for service providers.
- The increase in using online identities also has a variety of societal impacts.

Background

A recent Government report entitled 'Future Identities' summarised the possible impacts of technologies on the meaning of identity and the consequences for society, commerce and security. The report highlights that people often have several identities, online and offline and that the boundary between public and private lives online is increasingly becoming blurred.[1]

An increasing number of interactions, transactions and services are conducted online. Social media such as Facebook (used by half of the UK's population) and Twitter have changed the way people interact with each other. Online retail and financial services provide a virtual high street, with an average weekly turnover of £711m. Many public services are now online, from registering on the electoral roll to booking medical appointments. Using any of these services requires an individual to establish one or more online identities.

Internet Accessibility and Use in the UK

Increased use of online services is a consequence of:

- access to reliable, fast, ubiquitous broadband internet
- cheaper connection costs
- access to mobile internet, using smartphones and other portable devices.

The UK is one of the most online countries in the world,[2] with internet access available across the vast majority of the country. In 2012, 80% of UK households had internet access, up from 77 % in 2011.[3] The amount of time spent online has risen steadily in recent years (from 10 hrs per person, per week in 2005 to 15 hrs in 2011). However, some groups remain excluded from using the internet and participating in online activities.

Cybercrime

The rise in the use of online services has been accompanied by an increase in cybercrime including identity fraud and other risks associated with using sensitive and personal data online. Statistics on the scale and the economic impact of cybercrime vary considerably.

- A Home Office report estimated that cybercrime costs the UK economy £27bn a year.[4] This figure received widespread scepticism. Other analyses estimate that annual direct losses are significantly lower.[5]
- 27.9% of UK adults are known to have been a victim of identity fraud at some point.[1]
- 9.4% of UK adults were a victim in 2011, losing an average of £481 each. However, many such costs are usually borne by financial institutions and businesses.[1]

As a consequence of the rise in online activities and cybercrime, a critical challenge is to provide secure, reliable

ways to authenticate identity so that people have confidence in the services they use. Similarly, organisations need to verify users' identity to fulfil regulatory requirements, manage commercial risk and protect users.

The Government Digital Service, part of the Cabinet Office, has the task of enabling digital access to public services. A new initiative is the Identity Assurance Programme (IDAP) which is developing a new way for citizens and businesses to assert their identity to Government, discussed later.

Creating and Using an Online Identity

Information Used

Identity need not be an absolute concept. Different degrees of personal information can be used according to the value or sensitivity of a transaction. Almost all online activities require disclosure of various personal data to create an online identity in order to use a service. Services include email, social networking, public services, e-commerce, banking, gaming and gambling, employment search, education and online courses. Identity is usually verified by establishing something you:

- know (password, PIN number)
- have (passport, bank account electronic security key)
- are (biometrics, measurements or unique physical or behavioural characteristics, such as DNA, iris or voice patterns).

When at least two of these elements are used together a stronger profile can be asserted for the individual. Online profiles link pieces of information that together uniquely identify an individual on the internet. The risks of placing too many personal attributes online that could be widely viewed are considered on page 4. The level of detail required depends on the nature of the service and the extent to which verification of identity is required by the service provider. For example, a municipal waste collection service may only need a person's address, not information about age, gender or marital status. High security systems requiring a larger number of detailed pieces of personal or sensitive identifying data are required for transactions like online banking. Secure online systems with sign-in procedures allow individuals to authenticate their entitlement to perform a certain task and to authorise transactions and data access by other parties.

Service providers need confirmation that users have been verified to ensure that they are entitled to the service they are requesting. Identity is verified by comparing the evidence supplied by the user with data available about them from trusted sources like credit providers, phone companies or employers. This is the basis of the government's new IDAP programme, outlined in detail later.

Verifying Online Identity

Online interactions are rapidly replacing face-to-face transactions, with a connection between a secure web server and an online identity containing a series of personal data attributes. Secure websites like online banking sites often hold large amounts of personal data attributes about their users. A complete profile of a person or organisation can be built up from separate pieces of information about them.

The requirements of what constitutes sufficient identification for many transactions, especially those conducted online, have changed. Previous approaches demanded disproportionately high levels of assurance. However a new approach, which only uses necessary credentials of a person's identity (proportionate to the risks associated with the service) is gaining popularity.[6] One approach is to provide third-party services which validate identity credentials in a transaction between a user and a service provider. This means that a user can perform transactions without having to disclose full identifying information to the service requesting data about their identity. Anonymous credentials allow a person to establish his or her right to perform a transaction without providing unnecessary personal data.

UK Government's Identity Assurance Programme

Many public services are managed and delivered via online interfaces. This is part of the new 'Digital by Default' model for government services. POSTnote 321, 'E-Democracy,' discusses opportunities and issues surrounding the use of online services by government agencies. The Government Digital Service's Identity Assurance Programme (IDAP) is developing a new way for people in the UK to assert their identities to access government services online.

The IDAP's model means that people will assert their identity to government via private sector identity providers (Box 1). This avoids large scale, centralised government storage of personal information. The identity providers will collect and validate the necessary evidence of each user's identity, with their consent. Once their identity is registered, a user will then be able to authenticate with the identity provider in order to access online government services. For example, users requesting a service from a public authority might use their online banking credentials to authenticate to their bank, which can in turn vouch for their identity to the public authority. This approach avoids the cost, inconvenience and privacy risks associated with registering and managing a population of identities. The IDAP is intended to support fraud prevention and increase efficiency by reducing paperwork and costs of providing services to individuals and businesses. Key features of the identity programme are that it must:

- be designed around the user
- be both private and secure
- establish a common level of security and trust between users, identity providers and Government.

Implementing Identity Services across Government

Identity assurance services will be implemented across Government, as required. Notably, early pilots are taking place in HM Revenue and Customs and the Department for Work and Pensions (DWP). In late 2012, DWP announced that IDAP's identity assurance model will be incorporated

into the Universal Credit framework.[7] Universal Credit will allow benefit claimants to make a claim and manage their account online. The Universal Credit benefit programme is aimed at making the benefit system simpler and clearer for beneficiaries. The DWP expects that most claimants will manage their benefits online. Provision will be made so that those without internet access can use facilities in high street outlets and job centres or receive help by telephone.

Box 1. Government Identity Programme Providers
Eight providers have been announced: PayPal, Post Office, Cassidian, Digidentity, Experian, Ingeus, Mydex and Verizon. In future, as more companies are certified to become identity providers, it is intended that identity provision will become an open market commercial opportunity for identity providers. It is hoped that this will drive down the cost of identity provision to Government.

Security of the Identity Assurance Programme
Privacy and security are key concerns of the Identity Assurance Programme. The IDAP is developing a model which aims to address these concerns. It is engaging with an independent Privacy and Consumer Advisory Group comprising external stakeholders to work on this issue. It is also working with the Government's National Technical Authority for Information Assurance to ensure that the model meets security requirements.

The following section looks at how using online identities can be secured and the technologies used. Box 2 gives an overview of the legislation relevant to personal data.

Box 2. Privacy of Personal Data: Legislation
In most cases personal data collected online is protected under the laws of the country hosting the website. It may also fall under additional jurisdiction of the country where the site is being accessed. The two principal pieces of UK legislation are the Data Protection Act (1998), which is the UK interpretation of the EU Data Protection Directive (1995), and the Electronic Communications Act (2000). The law stipulates that personal data may only be stored for a specified period of time and only with consent. As the amount of personal data provided and used by individuals online increases exponentially, there is debate about the ownership of personal data. In 2012, the European Commission proposed a reform of the 1995 Directive to meet modern demands for data handling online. Proposed reforms intend to give users more control over their personal data

Security of Online Identity

Security Technology

There are several methods to protect identity and data online. As well as passwords, service providers may issue users with specialised hardware such as an electronic key in order to access online banking. The key generates a unique code for each transaction the user makes. Another method is using on-screen keyboards to prevent key-stroke-copying viruses and malicious software accessing accounts by storing passwords.

Perceptions of Security, Privacy and Anonymity

A challenge in providing online security is not only ensuring that security measures appropriate to the transaction are in place but also making users feel safe when using an online service. They can be addressed through recognisable processes of passwords and verification, as well as the presence of clear symbols by trusted security providers on secure websites, such as Paypal and 'Verified by Visa'.[8] Security and trust is key to e-commerce in order to retain customers and business partnerships. Some data on users' perceptions of privacy, anonymity and security are outlined in Box 3. However, individuals' online behaviour and habits do not necessarily reflect the concerns that they express when they are surveyed about conducting online activities.

Box 3. Perceptions of Online Personal Information Security
A large academic study (the VOME project) has collected data on attitudes and behaviours regarding online identity, consent and privacy.[9] The most common concerns about using online identities reported in the study were:

- identity fraud
- credit card numbers being obtained and intercepted by someone else while shopping online
- strangers obtaining personal information
- incorrect credit card charges when shopping online
- computer viruses sending out emails in their name.

Over a quarter of the people surveyed said they were "very concerned" about their privacy online. Just over half were "not too concerned" about family, friends and people whom they know acquiring their personal information. However, one third of those surveyed said they were "very concerned" about businesses and people they do not know acquiring their personal information. Notably, only a third of those surveyed believed that online sites would honour their privacy policies. Half those surveyed thought that the tracking of web sites visited by users was harmful.

National Jurisdictions Online

Current UK and EU legislation on data protection is outlined in Box 2. A recent example of non UK-based websites having to comply with local laws is Facebook's facial recognition function used on users' photographs. This function stores biometric data of an individual's facial features and links these with that person's name and user data, often without explicit consent of the person. The storage of this kind of non-essential data for an unspecified length of time has come under scrutiny in several European countries. Inquiries in Ireland, where Facebook's European operations are based, Germany and Norway have led to the facial recognition feature being altered or completely blocked from European access to the site.

Impacts of Online Identity Use

The rise in the use of online services offers numerous potential benefits such as increasing choice and convenience for users, improved accessibility to services and reduced costs. However, there are risks and societal impacts at both the individual and national level.

Benefits

Managing who can access personal data is one of the major benefits of personal control over online data and identity. Online accounts may be used by a person or company to identify who may see data, what they may see and what they may use it for. This control supports a shift in many companies and government offices to a 'digital by default'

model for connecting with customers. An example is the proposals to move to an online application system for administering DWP's new Universal Credit benefit programme. Online accounts provide a convenient and secure method by which organisations can manage authorisation of who may conduct specific transactions. Control over personal data online helps the user protect their data and discover if their data has been accessed or used without permission.[8]

The IDAP benefits Government because it avoids the cost of storing and managing large amounts of data, as well as the cost and inconvenience associated with registering users and supporting their accounts. By using existing secure sign-in systems, Government will not need to handle the customer service concerns of managing its own online sign-in systems, such as lost passwords and storage of redundant information. Benefits to users are a reduced risk of fraud, increased convenience and reassurance that they are interacting with a bona fide service. If the current initiatives can boost trust in online services, then Government is likely to make substantial savings through online delivery. It might also help to provide digitally marginalised users with the confidence they need to use online services.

Risks

Security vulnerabilities of online services and poor management of personal online security by individuals make them a target for criminal activity. When people place large amounts of personal data online (such as birth date or mother's maiden name on a social networking site), this can undermine the security of online personal transactions which require these details for verifying identity. This data may be easily obtained from social networking sites and can reveal attributes of identity which may be used for criminal activity. Furthermore, risks of unwanted access to or theft of personal data can include theft of entitlements, such as benefits, access to sensitive documents and accounts and identification of the person behind a username. Lack of effective enforcement in some countries has led to cybercrime which is difficult to trace.

A key consideration of the risk of performing online transactions with online identities is the difference between authentication of a user and authentication of a transaction. It is important that the user is aware of the transaction being performed, and is only performing the transaction he or she originally intended. A common form of cyber-crime is the interception of valid transactions to reroute information, data or money. A secure online identity does not necessarily mean that the online service is secure. Some suggest that online delivery of services, such as universal credit, potentially opens more potential avenues for fraudulent claims or coercion from family members or others to grant access to benefit money. A persona that an identity portrays may not be the individual who benefits from the service.

Societal Impacts

There is increasing research interest in the social impact of online interactions between individuals and groups. A recent study suggests that reduced self-awareness and a belief in anonymity when interacting with others online can lead to anti-social behaviour online which would be unlikely or unusual in a face-to-face setting.[10] There is also concern that a widening gap between regular internet users and those who are unable or unwilling to participate in online services will result in unequal access to public services. Educational initiatives taught in secondary schools and 'Get Safe Online,' aimed at a wider audience, intend to educate users about online safety and the steps they can take to protect personal information online.

Personal Legal Implications

The legal implications of agreements or statements made online are varied and, in many cases, unclear to the user. Recent cases of legal action taken against Twitter and Facebook users over threatening or offensive remarks posted on social media sites have highlighted the emerging phenomenon of cyber-bullying and its consequences. The Director of Public Prosecutions has called for "an informed debate about the boundaries of free speech in an age of social media". Consumer reports have called for simplification of 'fine print' terms and conditions pages to more digestible formats for users. Google has made attempts to simplify its fine print by creating an all-in-one policy covering most of its services, including search, YouTube, Picasa, Chrome and Android.[11]

Managing Personal Information Online

Users' trust in social networking services has been undermined by changes to terms and conditions in how their personal data is stored and for what purposes it can be used. For example, the photo sharing site Instagram (owned by Facebook) was criticised by users for changing its terms and conditions, appearing to allow the site to sell users' data and photos without permission or acknowledgement of the user. Instagram quickly responded with a change in terms and conditions and an open letter apologising to users for confusion caused over photo ownership on the site.[12] Another photo-sharing service, Flickr (owned by Yahoo) has responded to users' demands by only selling photos with the explicit permission of the photo's owner and sharing profits with the owner.[13]

Endnotes

1 *Future Identities*, Foresight 2013
2 http://thewebindex.org/
3 *Internet Access Quarterly Update, Q3,* Office for National Statistics, 2012
4 *The Cost of Cybercrime*, Cabinet Office and Detica, 2011
5 Anderson, R., et al. *Measuring the Cost of Cybercrime*. 11th Workshop on the Economics of Information Security, 06/2012
6 Paquin, C. *U-Prove Technology Overview*, Microsoft, 2011
7 www.dwp.gov.uk/newsroom/press-releases/2012/nov-2012/dwp118-12.shtml
8 *People Feel Safe on the Internet*, Amsterdam Internet Exchange, 2012
9 Coles-Kemp, L. et al., *Privacy on the Internet*, VOME, 2010
10 Wilcox, K. & Stephen, A., *Are Close Friends the Enemy?,* J. of Cons. Res. 2004
11 Parris, R., *Online T&Cs longer than Shakespeare plays...*, WHICH?, 2012
12 http://blog.instagram.com/post/38252135408/thank-you-and-were-listening
13 Arthur, C., *Facebook forces Instagram users... photos*, The Guardian, 2012